UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

MEDIDATA SOLUTIONS, INC., et al.,		
Plaintiffs,	:	17 Civ. 589 (LGS)
-against-	:	**OPINION AND ORDER**
VEEVA SYSTEMS INC.,		
Defendant.	:	

LORNA G. SCHOFIELD, District Judge:

Plaintiffs Medidata Solutions, Inc. and MDSOL Europe Limited (collectively, "Medidata") bring this action against Veeva Systems Inc. ("Veeva") alleging a violation of the Defend Trade Secrets Act (the "DTSA") and various New York common law claims. Defendant moves to dismiss the Second Amended Complaint (the "Complaint"). For the reasons below, the motion is denied.

I. BACKGROUND

The following facts are taken from the Complaint and assumed to be true only for the purpose of this motion. *See Littlejohn v. City of New York*, 795 F.3d 297, 306 (2d Cir. 2015).

A. Plaintiff's Growth and Trade Secrets

Founded in 1999, Plaintiff is a New York-based software company offering software-as-a-service ("SaaS") solutions that allow life science companies to design, manage and evaluate clinical trials. Plaintiff released its first software product in 1999, an electronic data capture ("EDC") system that allowed clients to collect data in electronic rather than paper form. In 2011, Medidata acquired a company that developed clinical trial management software ("CTMS"), improved the product and added it to its software suite. Throughout its existence, Medidata has

continued to develop and merge software used at different aspects of clinical trials into a uniform interface for the benefit of its clients. In 2013, based on its understanding of client needs, Plaintiff introduced Medidata Clinical Cloud, a product that addressed every aspect of the clinical trial process "from concept to conclusion." Since 2008, Medidata has spent over $500 million in research and development. By 2015, nine of the top ten selling drugs globally were developed using Medidata's technology.

In connection with these operations, the Complaint alleges that the following are Medidata's trade secrets:

1. Clinical trial software solutions: information regarding its activity-driven design model and product design principles, software architecture and design, product roadmaps, functionality requirements relating to platform integration across software modules, and clinical trial management tools (including without limitation study design, start-up, strategic monitoring, and analytics functionalities),
2. Sales and marketing activities: information regarding customer profiles and segments, "early adopter" customers, historical pricing data, pricing projections, pricing formulae and methodologies across product offerings, product development priorities and pipelines, unannounced products, product release timelines, and industry competitive intelligence, and
3. Short- and long-term business plans: strategies concerning marketing, sales, research and technology initiatives, go-to-market strategies, emerging growth areas and opportunities, and geographic/customer expansion opportunities and projections for each of the solutions that it offers.

The Complaint alleges that these trade secrets contain proprietary information that helped Medidata retain a competitive advantage in the industry.

To protect these trade secrets, Medidata took several measures. First, Medidata required customers, partners and vendors to sign non-disclosure agreements and provided them with minimum access to confidential information. Employees also entered into confidentiality and non-compete agreements. The confidentiality agreements prohibited employees from sharing information about "research, product plans, products, services, customer lists and customers . . . , markets, software, developments, inventions, processes, formulas, technology, designs,

drawings, engineering, hardware, configuration information, marketing, [and] finances." The agreements also prohibited employees from retaining Medidata documents upon leaving the company. Medidata's Corporate Policy Manual states that employees are prohibited from making unauthorized transmissions of Medidata files through the company's email system. Medidata also protects its electronic information through two-factor authentication and limits the internal distribution of materials to employees on a need-to-know basis.

B. Veeva's Actions

Veeva is a cloud-computing software technology company founded in 2007. The company is headquartered in Pleasanton, California, but also has offices in New York. In 2008, Veeva launched its core product, a customer relationship management app, which accounted for the majority of Veeva's revenue. In 2016, Veeva launched a cloud-based content management platform for life science customers. Although Veeva is a software company, it has no experience developing products that manage clinical trials across different stages.

Veeva hired many of Medidata's former employees. In 2014, a Senior Product Manager, Sondra Pepe, left Medidata to join Veeva. In 2015, Medidata's Executive Vice President of Field Operations, Alan Mateo, left Medidata and promptly joined Veeva. Veeva has given Mateo above-average compensation, including $11.5 million in stock options that he exercised during the first two and a half years of his employment. In 2016, three senior Medidata executives -- Michelle Marlborough, Vice President of Product Strategy; Richard Young, Vice President, Global Consulting Partners; and Jason Rizzo, Vice President of Product Sales -- left for Veeva. These employees were and remain intimately involved in product development and sales in their current and former job roles. Mateo and Marlborough continued to work in New York after they joined Veeva.

Days before her departure from Medidata, Pepe sent emails to her personal email address that included detailed information about Medidata's CTMS product development process. Similarly, on May 19, 2016, two months before leaving Medidata, Marlborough used her Medidata email account to send sensitive information to her personal email, including documents that contained information about Medidata's 2014 product roadmap. Mateo also accessed a file containing Medidata's confidential sales data and sales targets while he was employed at Veeva. On June 27, 2017, Medidata found out that four of these employees -- Pepe, Mateo, Marlborough, and Rizzo -- retained 3,100 key company documents, many of which were marked "Private and Confidential," after their departure to Veeva.

On June 22, 2016, Veeva announced its first CTMS offering, and on October 13, 2016, Veeva announced its first EDC offering. These products were marketed as part of Veeva's "Clinical Suite," a "suite of unified cloud applications to streamline clinical operations and data management, from study startup to archive." On October 18, 2018, at Veeva's Global R&D Summit, Marlborough touted Veeva's CTMS as a "single source of truth across clinical operations," language which closely mirrored discussions Marlborough had during meetings while still at Medidata in which Medidata's short-term strategy goals were discussed. After Veeva's product announcements, Medidata's investors asked Medidata representatives specific questions about its product offerings that demonstrated knowledge of confidential information known only to senior employees at the company. When Medidata representatives asked about the source of the questions, the investors' responses uniformly indicated that Veeva disseminated the information and prompted them to ask the questions.

II. STANDARD

To survive a motion to dismiss, "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* (citing *Twombly*, 550 U.S. at 556). It is not enough for a plaintiff to allege facts that are consistent with liability; the complaint must "nudge[ ] their claims across the line from conceivable to plausible." *Twombly*, 550 U.S. at 570. "To survive dismissal, the plaintiff must provide the grounds upon which his claim rests through factual allegations sufficient 'to raise a right to relief above the speculative level.'" *ATSI Commc'ns, Inc. v. Shaar Fund, Ltd.*, 493 F.3d 87, 98 (2d Cir. 2007) (quoting *Twombly*, 550 U.S. at 555). On a Rule 12(b)(6) motion, "all factual allegations in the complaint are accepted as true and all inferences are drawn in the plaintiff's favor." *Apotex Inc. v. Acorda Therapeutics, Inc.*, 823 F.3d 51, 59 (2d Cir. 2016).

III. DISCUSSION

A. Defend Trade Secrets Act Claims

To state a claim for trade secret misappropriation under the DTSA, a plaintiff must plausibly allege that (1) it possessed a trade secret, and (2) the defendant misappropriated the trade secret. 18 U.S.C. §1836(b)(1). The Complaint sufficiently alleges the trade secrets at issue and that Defendants misappropriated them.

1. DTSA Trade Secret

Under the DTSA, the term "trade secret" includes "all forms and types of financial, business, scientific, technical, economic, or engineering information" if (1) "the owner thereof

has taken reasonable measures to keep such information secret" and (2) "the information derives independent economic value . . . from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information." 18 U.S.C. § 1839(3). Although the Second Circuit has not expressly articulated a specificity requirement, district courts in this circuit routinely require that plaintiffs plead their trade secrets with sufficient specificity to inform the defendants of what they are alleged to have misappropriated. *Big Vision Private Ltd. v. E.I. DuPont De Nemours & Co.*, 1 F. Supp. 3d 224, 258 (S.D.N.Y. 2014) (collecting cases), *aff'd sub nom. Big Vision Private Ltd. v. E.I. du Pont de Nemours & Co.*, 610 F. App'x. 69 (2d Cir. 2015) (summary order).

The Complaint sufficiently identifies the trade secrets at issue. It specifies numerous specific categories of information relating to its software, marketing and business plans. These allegations give Defendants adequate notice as to what the misappropriation allegations concern. *See Tesla Wall Sys., LLC v. Related Cos., L.P.*, No. 17 Civ. 5966, 2017 WL 6507110, at *9 (S.D.N.Y. Dec. 18, 2017).[1] *Compare, e.g.*, *PaySys Int'l, Inc. v. Atos Se*, No. 14 Civ. 10105, 2016 WL 7116132, at *10 (S.D.N.Y. Dec. 5, 2016) (holding the complaint was insufficiently specific when the trade secrets were identified as "the Products, all Enhancements to the Products and all proprietary information, data, documentation and derivative works related to the Products") *with Tesla Wall*, 2017 WL 6507110, at *9 ("Tesla's complaint is highly specific regarding

[1] The Second Circuit has not yet addressed the DTSA in a reported opinion. As the requirements are similar for showing a misappropriation of a trade secret under the DTSA and misappropriation under New York law, *Free Country Ltd. v. Drennen*, 235 F. Supp. 3d 559, 565 (S.D.N.Y. 2016), district courts often rely on SDNY cases discussing misappropriation under New York law to analyze DTSA claims. *See, e.g.*, *Elsevier Inc. v. Doctor Evidence, LLC*, No. 17 Civ. 5540, 2018 WL 557906, at *4 (S.D.N.Y. Jan. 23, 2018); *In re Document Techs. Litig.*, 275 F. Supp. 3d 454, 461–62 (S.D.N.Y. 2017); *Drennen*, 235 F. Supp. 3d at 565.

defendants' course of conduct[and] pleads numerous specific categories of information, such as 'technical data, internal pricing information, work product, research, engineering designs,' etc. . . . .").

The Complaint also pleads that Plaintiffs took reasonable steps to protect the trade secrets. Medidata required its customers, partners, vendors and employees to enter into non-disclosure agreements and prohibited its employees from making unauthorized email transfers of company documents and from retaining company documents after their employment ended. Medidata also restricted access to information to those with a need to know by using passwords and, for some applications, two-factor authentication. These security measures are sufficient to allege that Medidata took "reasonable steps" to protect its trade secrets. *See Oneida Grp. Inc. v. Steelite Int'l U.S.A. Inc.*, No. 17 Civ. 0957, 2017 WL 6459464, at *7 (E.D.N.Y. Dec. 15, 2017) (holding that plaintiff took reasonable steps to protect its trade secret when third parties were required to execute nondisclosure agreements and employees were asked to do the same).

The Complaint plausibly alleges that the trade secrets derive independent economic value from being kept secret. The Complaint alleges that Medidata spent a great deal of time and money, $500 million, developing its technology, that Medidata went to great lengths to protect its confidential business information and that Medidata became an industry leader managing the clinical trials of 9 of the 10 top-selling pharmaceutical products in 2015. These allegations plausibly show that Medidata's trade secrets are valuable in part because they are secret. *See Bancorp Servs., LLC v. Am. Gen. Life Ins. Co.*, No. 14 Civ. 9687, 2016 WL 4916969, at *11 (S.D.N.Y. Feb. 11, 2016) (applying New York law) (plaintiff plausibly pled trade secret when it had a proprietary account methodology that it took steps to protect and spent millions to develop).

2. DTSA Misappropriation

Under the DTSA, "a party must show an unconsented disclosure or use of a trade secret by one who (i) used improper means to acquire the secret, or, (ii) at the time of disclosure, knew or had reason to know that the trade secret was acquired through improper means, under circumstances giving rise to a duty to maintain the secrecy of the trade secret, or derived from or through a person who owed such a duty." *Elsevier*, 2018 WL 557906, at *3 (internal quotation marks omitted); *see also* 18 U.S.C. § 1839. In other words, the defendant misappropriates a trade secret (1) when it acquires a trade secret by improper means, or (2) discloses or uses the trade secret without consent. *AUA Private Equity Partners, LLC v. Soto*, No. 17 Civ. 8035, 2018 WL 1684339, at *4 (S.D.N.Y. Apr. 5, 2018) (citing 18 U.S.C. § 1839(5)). "Improper means" under the DTSA can involve "inducement of a breach of a duty to maintain secrecy," 18 U.S.C. § 1839(6)(A), including contractual agreements not to disclose or disseminate information, *Broker Genius, Inc. v. Zalta*, 280 F. Supp. 3d 495, 511 (S.D.N.Y. 2017).

The Complaint sufficiently alleges that Veeva misappropriated Medidata's trade secrets. The Complaint alleges that several of Medidata's high level employees had access to Medidata's trade secrets, retained Medidata's documents marked "Private and Confidential" upon joining Veeva, sent documents containing trade secrets to their personal emails close to their departure from Medidata to join Veeva, and, in one circumstance, actively accessed a Medidata file while working for Veeva. The Complaint alleges that five senior members of Medidata -- all of whom went on to work for Veeva -- thereby breached Medidata's policies and their employee confidentiality agreements. Regarding Alan Mateo, who was Medidata's Executive Vice President of Field Operations and joined Veeva in a comparable position, the Complaint alleges that Veeva incentivized him to disclose Medidata's trade secrets by paying him an outsized

compensation package; Mateo cashed out $11.5 million dollars in stock options after about two and a half years at Veeva. These allegations plausibly suggest that Veeva hired Medidata employees and induced them to breach their confidentiality obligations to Medidata by divulging trade secrets.

The Complaint also sufficiently pleads that Veeva misappropriated Medidata's trade secrets by obtaining them and using them. The Complaint alleges that Veeva urged Medidata's investors, analysts, clients, prospective clients and partners to ask Medidata specific questions that relied on confidential information known only to high-level employees at Medidata. The Complaint also alleges that Veeva marketed and offered products with specific features and functionality that had been the focus of confidential research and technology initiatives at Medidata, and that Veeva used Medidata's trade secrets to introduce competing products in record time despite Veeva's lack of experience in developing SaaS technology for clinical trials. *See Medtech Prod. Inc. v. Ranir, LLC*, 596 F. Supp. 2d 778, 788–790 (S.D.N.Y. 2008) (applying New York law) (citing the plausibility standard and denying motion to dismiss when defendant was able to create a competing product on an "expedited basis" despite having no experience in the dental protector market). By contrast, Medidata released its CTMS system 12 years after launching its first SaaS technology for clinical trials and relying upon the knowledge of an acquired company that previously made the product. Taken together, these allegations plausibly raise an inference that Veeva misappropriated Medidata's trade secrets.

B. Choice of Law for State Law Claims

The Complaint asserts New York common law claims of misappropriation of trade secrets, tortious interference with contractual relations, unfair competition, aiding and abetting

breach of fiduciary duties and unjust enrichment. Defendant asserts that California law applies to any common law claims.

In tort actions, New York courts resolve conflicts of law by applying an "interest analysis" under which the law of the jurisdiction having the greatest interest in the litigation applies. *AroChem Int'l, Inc. v. Buirkle*, 968 F.2d 266, 270 (2d Cir. 1992) (applying New York law); *accord Mashreqbank PSC v. Ahmed Hamad Al Gosaibi & Bros.*, 12 N.E.3d 456, 460 (N.Y. 2014). In trade secrets cases, the Second Circuit and courts in this district have used the locus of the misappropriation to determine the state with the greatest interest in the litigation. *See Softel, Inc. v. Dragon Med. & Sci. Commc'ns, Inc.*, 118 F.3d 955, 968 (2d Cir. 1997) (using New York conflict-of-law principles to determine that New York law applies because, among other things, "the misappropriation, if any, apparently took place in New York"); *accord Sarkissian Mason, Inc. v. Enter. Holdings, Inc.*, 955 F. Supp. 2d 247, 254 (S.D.N.Y. 2013). "Because a choice of law analysis is fact intensive, courts [in this circuit] often decline to make a choice of law determination at the motion to dismiss stage." *Holborn Corp. v. Sawgrass Mut. Ins. Co.*, 304 F. Supp. 3d 392, 398 (S.D.N.Y. 2018); *Nostrum Pharm., LLC v. Dixit*, No. 13 Civ. 8718, 2014 WL 4370695, at *10 (S.D.N.Y. Sept. 2, 2014); *Smith v. Railworks Corp.*, No. 10 Civ. 3980, 2011 WL 2016293, at *6 n.12 (S.D.N.Y. May 17, 2011).

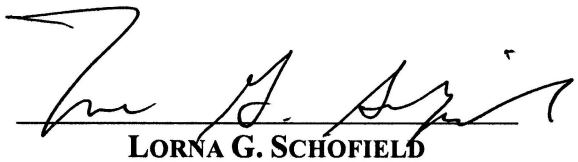
The Complaint does not allege the locus of the misappropriation, and engaging in a choice of law analysis is premature and unnecessary at this stage. Regardless of whether California or New York law applies, a state law claim arises from the facts alleged. Deciding the choice of law question at this stage would not alter the basic scope of discovery, and discovery on the state law claims may be entirely cumulative of the federal claim. Therefore, the motion to dismiss the state law claims is denied without prejudice.

IV. CONCLUSION

For the foregoing reasons, Defendant's motion to dismiss is DENIED.

The Clerk of Court is respectfully directed to close the motion at Docket Number 104.

Dated: November 26, 2018
New York, New York



LORNA G. SCHOFIELD
UNITED STATES DISTRICT JUDGE